Set Task Electronic Template – Unit 11

Task A - Activity 1 Template: Risk assessment of the networked system

Risk severity matrix

Probability of threat occurring	Very likely	Medium	High	Extreme
	Likely	Low	Medium	High
	Unlikely	Low	Low	Medium
		Minor	Moderate	Major
	Size of the loss			

Assessment

Threat number.	1
Threat title.	Attack via remote administration tool
Probability.	Very Likely
Potential size of loss / impact level.	Major
Risk severity.	Extreme
Explanation of the threat in context.	RATs often use port scanning to identify vulnerable data, exploit vulnerabilities and gain access to take control of computers. If a port is discovered to be open (via pings) for a website to be accessed and data exchanged, then a hacker can disguise as that website (phishing) and gain access via the open port. This could lead the hacker to have full control of the system which will put the company in jeopardy as the hacker may be able to access "highly confidential information" where the company may have broken the The Data Protection Act of 1998 if the protection measures in place were not deemed protective enough. Remote administration tools are usually initiated via a .exe, so as a countermeasure to this issue, the firewall group policy within windows can prohibit all foreign executables that are not within the whitelist from being initiated.

Threat number.	2
Threat title.	Attack via infected links
Probability.	Very likely
Potential size of loss / impact level.	Major
Risk severity.	Extreme
Explanation of the threat in context.	The staff and guests using the network are susceptible to phishing via suspicious links, or those disguised as legitimate links. These could be delivered to them via spam emails or by clicking advertisements. By opening these suspicious links, files may be downloaded or they may unknowingly provide the website with personal data. A file being downloaded would put the system at serious risk as it could infect the system or hold it ransom if they had downloaded ransomware which would render the system useless until it was removed.

Threat number.	3
Threat title.	Address Resolution Protocol Poisoning
Probability.	Unlikely
Potential size of loss / impact level.	Extreme
Risk severity.	High
Explanation of the threat in context.	ARP poisoning is a form of man-in-the-middle attack where the attacker changes the Media Access Control address and attacks a local area network by changing the target computer's ARP cache with a counterfeit ARP request and reply packets. This changes the MAC address into the hacker's known MAC address so they can monitor their victim. Because the ARP replies are forged, the victim's packets are sent to the hacker first instead of its intended destination. As a result, both the user's data and privacy are compromised. By conducting an ARP poisoning attack, hackers can gain sensitive data from the targeted computer or cause a denial of service. Also, if the hacker copies the targets MAC address and internet configurations, they may gain access to the network on a level of access which would be prohibited, thus gaining access to files that are classified.

Threat number.	4
Threat title.	NFC card cloning
Probability.	Very Likely
Potential size of loss / impact level.	Extreme
Risk severity.	High
Explanation of the threat in context.	NFC is a vulnerable technology as card data can be copied within seconds which will allow unauthorised access to the main office space. If there are no safeguards in place for server access, then it could lead to the servers being compromised as the attacker has gotten past the electronic door control system. This would put the company in a dangerous position as their classified documents concerning the clients will be in possession of a hacker. Instead of using NFC, a biometrics scanner would be safer due to biometrics being more difficult to clone and the hacker would have to go to far greater lengths to compromise this heightened level of security.

Threat number.	5
Threat title.	Misconfigured firewall within router
Probability.	Likely
Potential size of loss / impact level.	Medium
Risk severity.	High
Explanation of the threat in context.	The firewall settings may still be on default so no blacklisting or whitelisting of ports/websites have been specified. This could leave the network vulnerable to attack where the network could

	be infiltrated via the ports which have been left open or phishing via websites that are intended to be malicious and infect the user with malware. Although the firewall will be useful to an extent by being on default settings, because new viruses and malware are discovered every day, it is important for the firewall definition to be updated so it knows what to recognise for quarantine purposes.

Threat number.	6
Threat title.	Employee Sabotage
Probability.	Medium
Potential size of loss / impact level.	Extreme
Risk severity.	Medium
Explanation of the threat in context.	If an employee was to sabotage the company it would prove fatal as they could leak secure documents and put the company in legal jeopardy where they would be breaking multiple regulations such as the data protection act of keeping data secure and in a private environment. They could also cause serious damage to the company if files were misplaced/deleted. This type of attack can be avoided by monitoring employees and telling them they are being monitored via a logging system to deter them from taking such action. Also vetting employees and their background before hiring using checks such as "DBS" which check for criminality will help the company to decide whether they will be a liability in terms of their character and what type of person they are. This would entail an employee risk assessment. Time restrictions of user access rights can be implemented where login will not work during a specific time so their login cannot be abused outside of work hours.

Threat number.	7
Threat title.	Unauthorised access of account
Probability.	Medium
Potential size of loss / impact level.	Extreme
Risk severity.	Medium
Explanation of the threat in context.	If someone was to gain access of another employee's account who had left their computer logged in or was away for a short time, they could cause harm to the company under another person's identity. This could be avoided by teaching employees about account security and to ensure they always lock their account if they leave their workstation. A timeout can also be applied to all accounts where if inactivity is detected, the operating system is automatically locked. This is a feature that can be found within the Windows operating system in power management or display options.

Threat number.	8
Threat title.	Mobile device infiltration
Probability.	Likely
Potential size of loss / impact level.	Extreme
Risk severity.	High
Explanation of the threat in context.	Mobile devices that are given access to the network could be used to conduct MITM type attacks where their aim may be a denial of service or to interpret packets to steal information. Or, if their device carry malware it could infect the system.

Threat number.	9
Threat title.	Unauthorised use of CAT6 data outlet (Ethernet)
Probability.	Unlikely
Potential size of loss / impact level.	Moderate
Risk severity.	Low
Explanation of the threat in context.	The CAT 6 data outlets could be compromised by an attacker leaving a device connecting to look for vulnerabilities in the networks. Because Ethernet is categorised as a broadcast system, every message sent out by any computer on a segment of ethernet wiring reaches all parts of that segment and potentially could be read by any computer on the segment. A network switch however reduces the succession of packet sniffing due to their intended functionality where their aim is to only forward packets to the port of the destination which helps to mitigate sniffing attacks. Some switches may have port security which means that the number of mac addresses allowed on each switch is limited and the switch can be configured to whitelist MAC addresses so unknown network devices will not work with them.

Threat number.	10
Threat title.	Misconfigured default gateway on access points and servers
Probability.	Likely
Potential size of loss / impact level.	Extreme
Risk severity.	High
Explanation of the threat in context.	If the default gateways are still on default manufacture settings then it would allow anyone within the network to modify the access point’s settings if the default gateway is generic which would cause serious issues for the users and time loss for the company. They would be able to change parameters such as the name (SSID), password, the algorithm specified for the password and many other options. This can be avoided by making sure the username and password is changed on every gateway to ensure security of the network.

Threat number.	11
Threat title.	Admin server visible to network users
Probability.	Likely
Potential size of loss / impact level.	Major
Risk severity.	High
Explanation of the threat in context.	The server will appear on the network and people knowing of its existence makes it more prone to attack as attackers may see it as a point of entry.

Threat number.	12
Threat title.	Misconfigured settings on WiFi
Probability.	Low
Potential size of loss / impact level.	High
Risk severity.	Low
Explanation of the threat in context.	If the staff WiFi has not been properly secured in terms of multiple layers of authentication such as enforcing a standard encryption like WPA2-TSK, then an attacker could potentially read data transmission on devices using the Wi-Fi network if it remains open. The staff Wi-Fi is especially vulnerable to this as opposed to the guest due to the staff dealing with more sensitive materials which could be classified. This can be prohibited by enforcing encryption with a secure socket layer portal which will lead to a validation login page.

Threat number.	13
Threat title.	Thievery of PCs and servers
Probability.	Unlikely
Potential size of loss / impact level.	Extreme
Risk severity.	Low
Explanation of the threat in context.	If thieves were to break in and steal network devices the costs of replacement and ensuring data security would cost the business a massive amount of money in terms of replacing the equipment and ensuring there were no data breaches. However, due to them being on the 18th floor of the building, they are less susceptible to a physical attack and breaking through the controlled doors may prove difficult. The business is likely to be empty at night and people will know of the number of devices inside the building, but a 20-floor building with multiple businesses can be assumed to have security guards onsite. CCTV cameras and posting signs that there is active CCTV on-site will deter thefts. Encryption will secure data in the rare event that data is stolen to ensure integrity of the data and that the business is compliant with data protection laws as their servers store sensitive client information. There could also be a locked cabinet for sensitive data like servers or storage devices which contain client data which warrant a higher level of protection.